**常用工具培训**

**（一）UltraEdit工具**

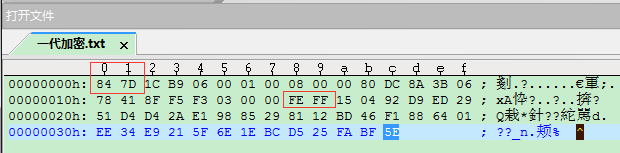
1、功能：

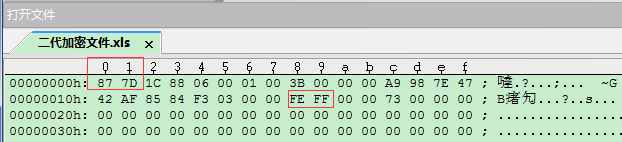
[1]可以查看加密文件是一代加密，还是二代加密；

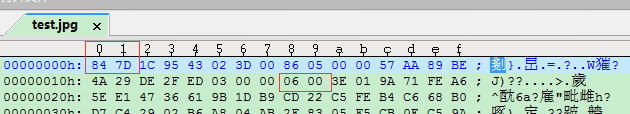
[2]可以查看加密文件是正式版加密的，试用版加密，是否有设置过企业密钥；

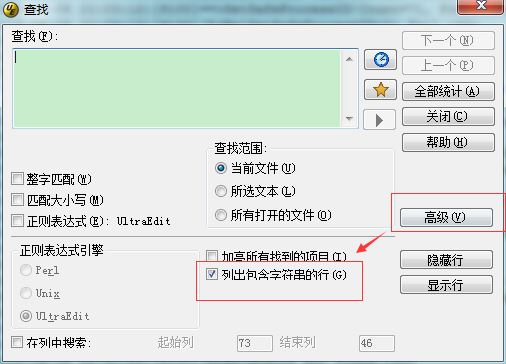
[3]可以查看日志。

2、使用说明：









**（二）绿盾调试工具**

1、功能：

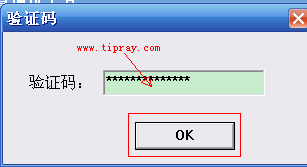
[1]可以获取终端运行日志；

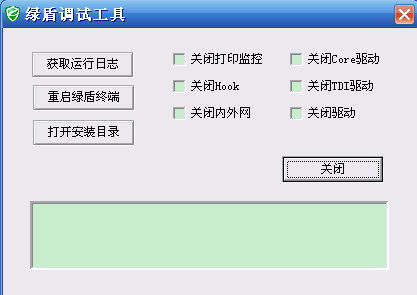
[2]可以重启终端进程；

[3]可以过滤绿盾组件排查问题。

2.使用说明：



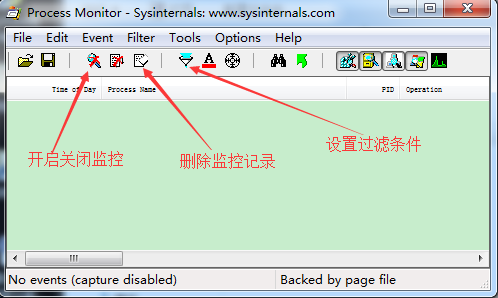


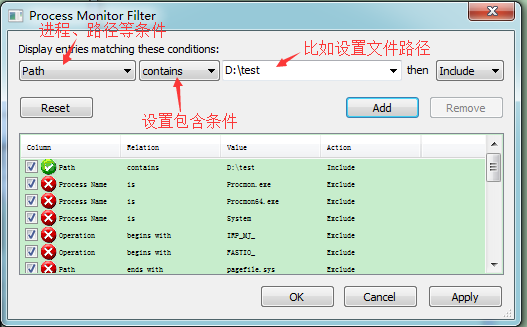


**（三）ProcessMonitor工具**

功能：监控文件操作日志

使用说明：

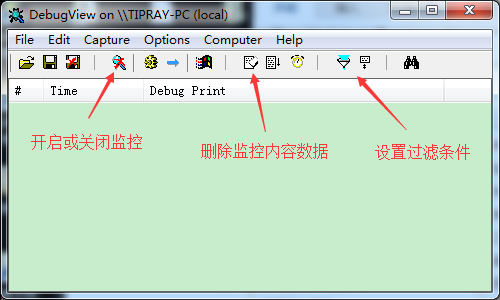




**（四）Dbgview工具**

功能：监控一些文件操作日志信息

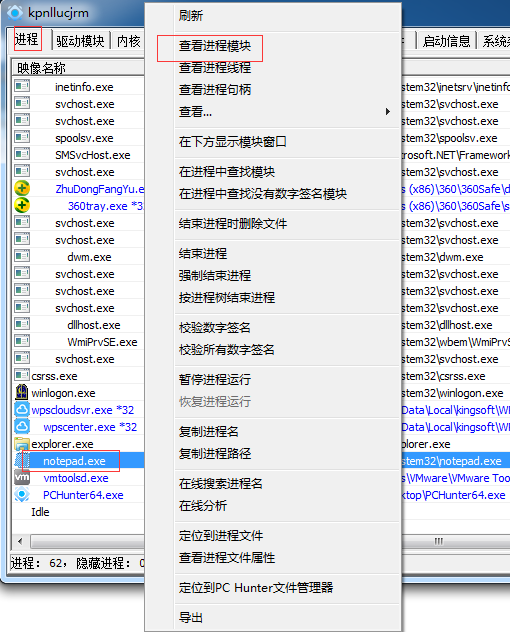
使用说明：

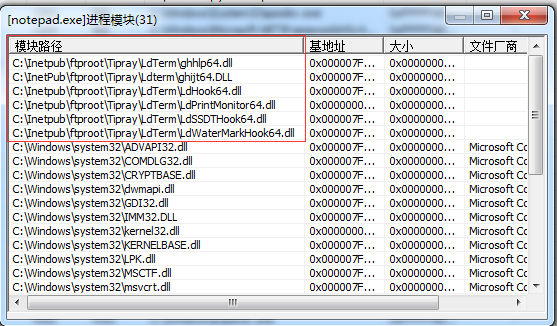


**（五）****PCHunter工具**

功能：查看驱动挂载、绿盾组件钩子挂载情况

使用说明：

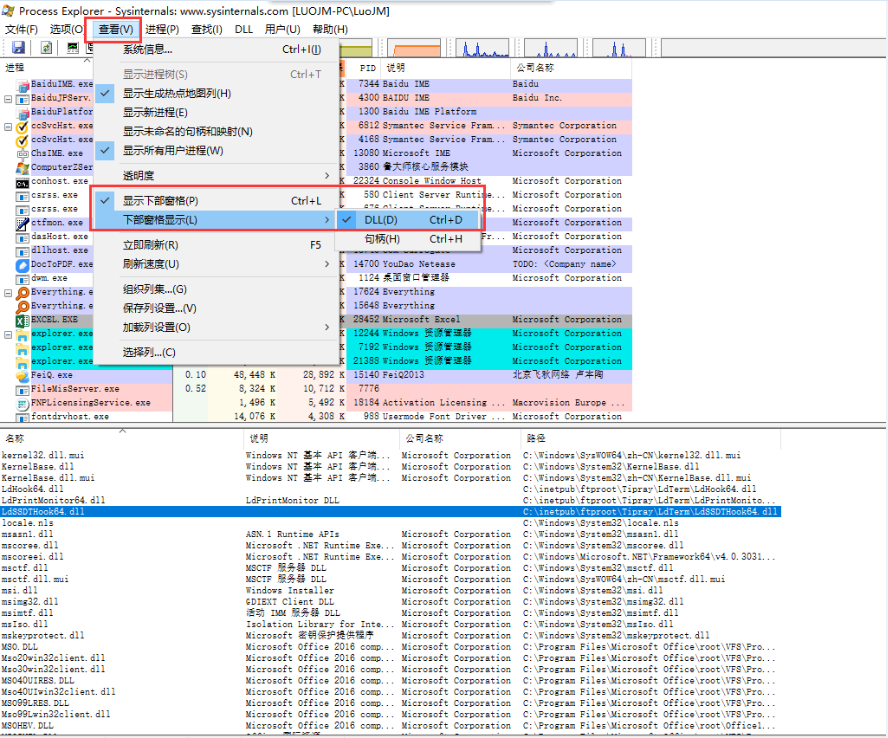




**（六）procexp64工具**

功能：绿盾组件钩子挂载情况

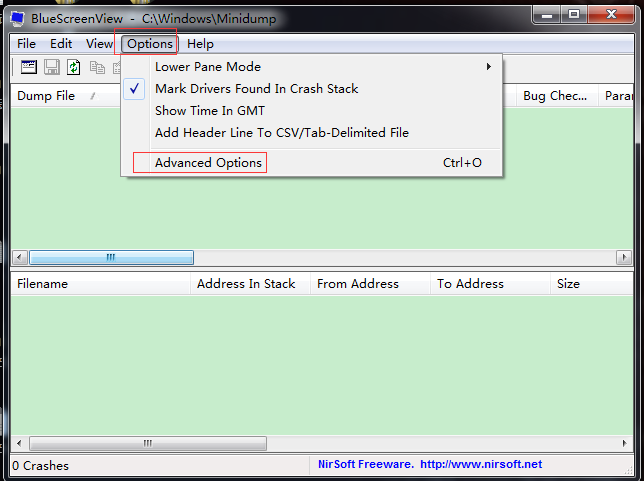
使用说明：

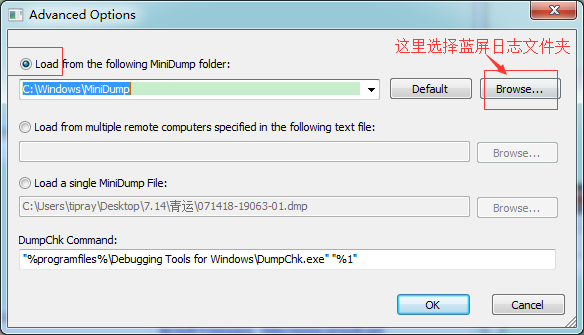


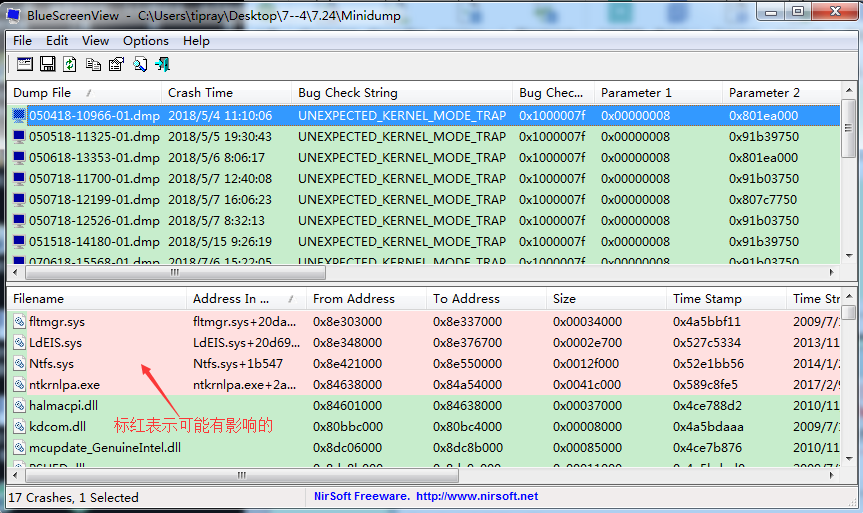
**（七）BlueScreenView工具或WinDbg工具**

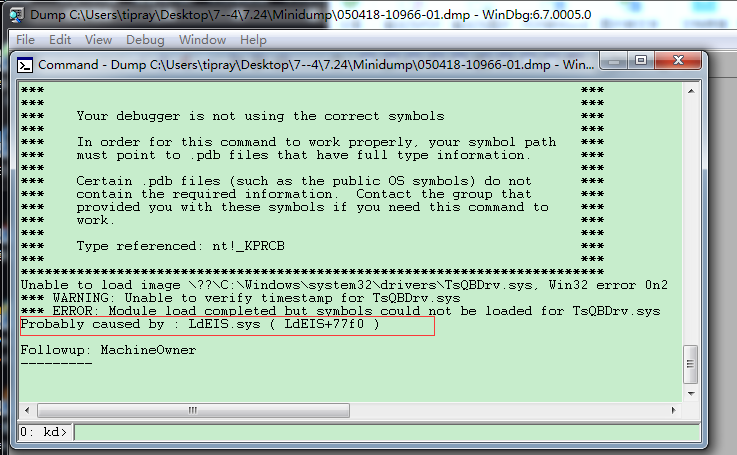
功能：查看蓝屏日志

使用说明：









**（八）wireshark工具**

功能：查看邮件白名单或服务器白名单上传协议和端口

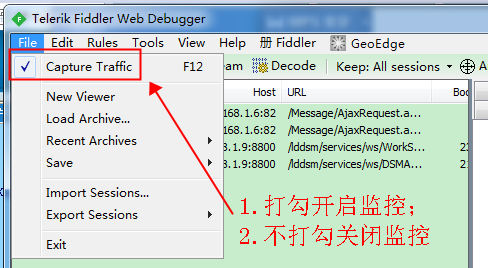
使用说明：

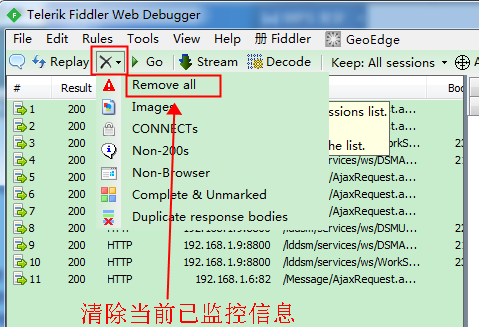
详见附件“wireshark工具查询邮件白名单以及服务器白名单注意事项”和“wireshark过滤条件的语法”

**（九）Fiddler工具**

功能：监控服务器白名单上传下载文件日志

使用说明：

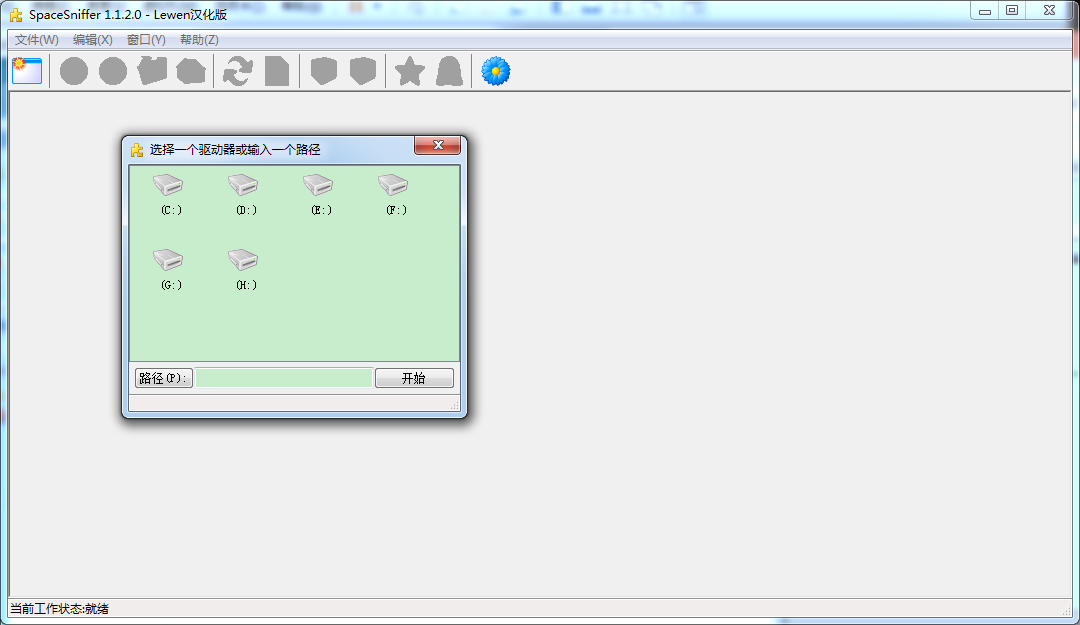


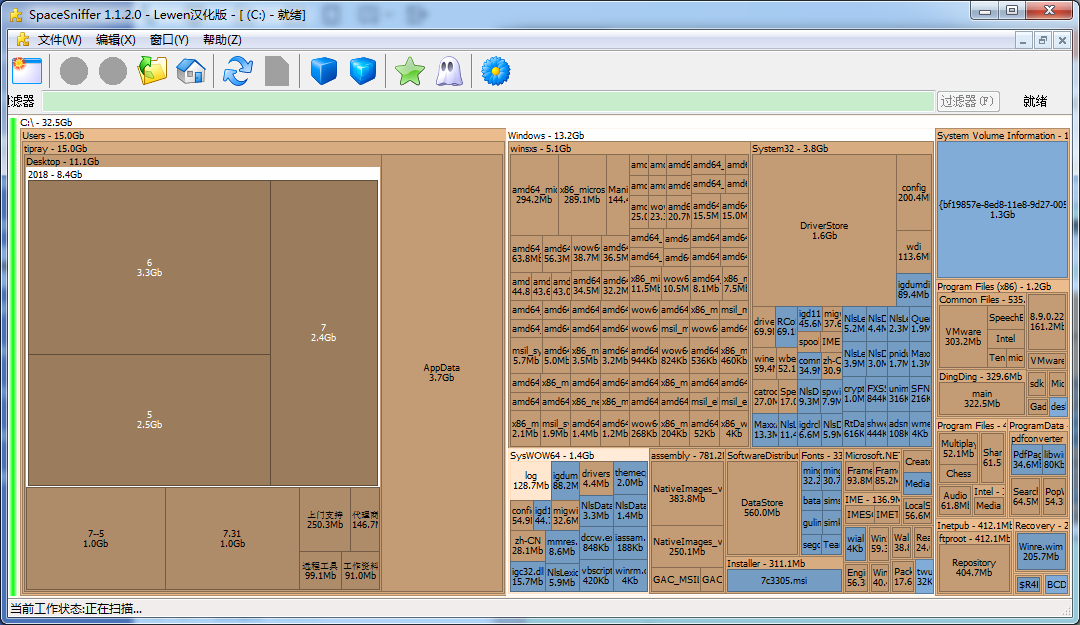


**（十）SpaceSniffer.exe工具**

功能：检查系统硬盘空间占用率（比如C盘无故空间变小，可以用它检查是哪个目录占用空间比较多，再选择性删除）

使用说明：





**（十一）365TCPView工具：**

功能：可以用于查看软件访问网络的数据走向，比如查看Foxmail发送邮件过程。

